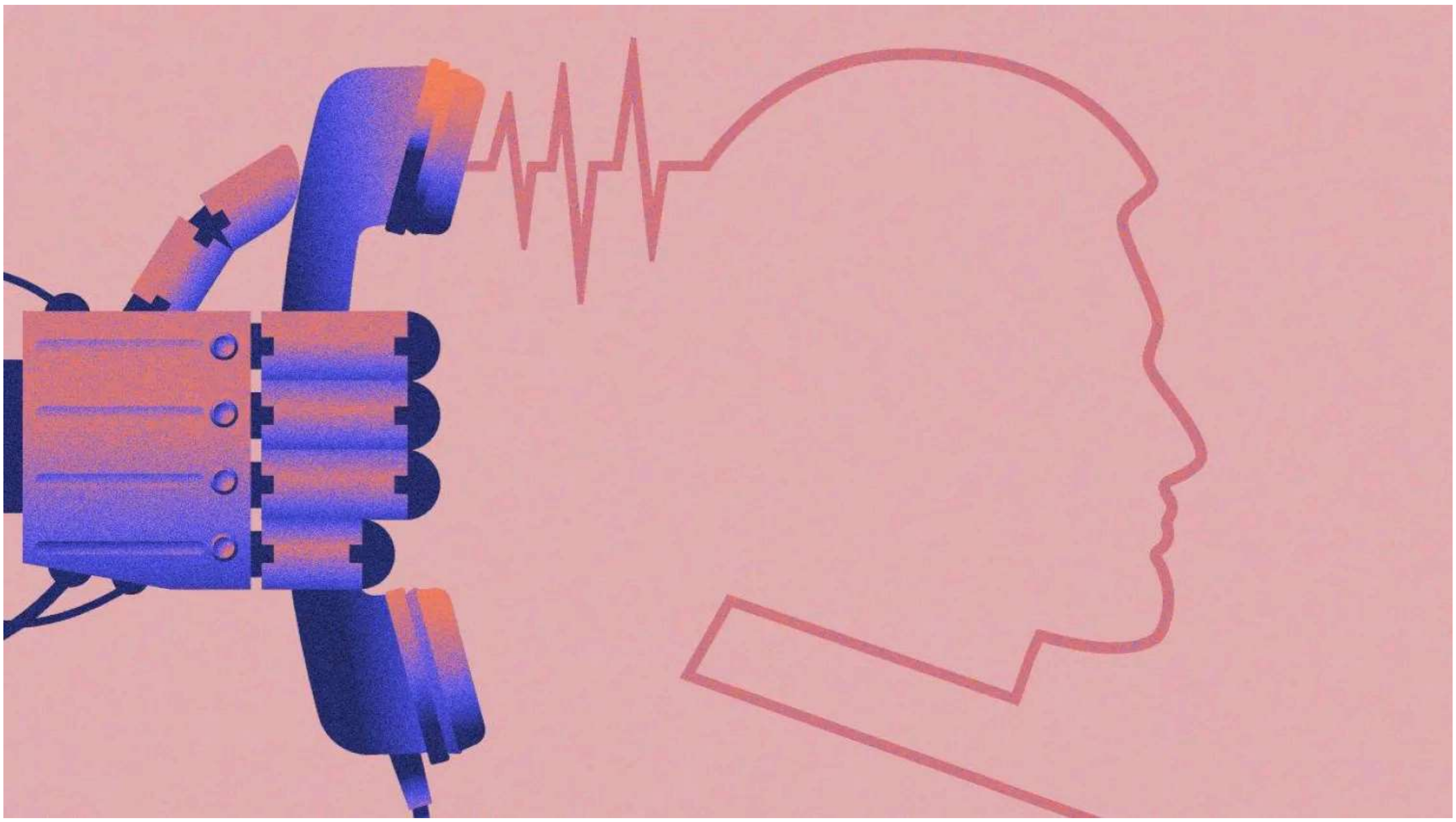
تكنولوجيا

مكالمات الاحتيال بالذكاء الاصطناعي... تزداد ذكاءً

شركات الاتصالات تطور الخطط للتصدي لها



واشنطن: «الشرق الأوسط»

نُشر: 13:18-8 مايو 2025 م . 11 ذو القِعدة 1446 هـ

تُحدث مكالمات الاحتيال ضجةً عالمية. ويُقدّر التحالف العالمي لمكافحة الاحتيال - The Global Anti Scam Alliance أن المحتالين سرقوا مبلغاً هائلاً قدره 1.03 تريليون دولار أميركي عالمياً في عام 2023، بما في ذلك خسائر ناجمة عن الاحتيال عبر الإنترنت، ومكالمات الاحتيال، كما كتب كولاولي صموئيل أديبايو(*).

الذكاء الاصطناعي والاحتيال

لطالما كانت المكالمات الآلية، والاحتيال عبر الهاتف مشكلةً تثير إحباطاً -وغالباً ما تكون خطيرة- للمستخدمين. والآن، يُفاقم الذكاء الاصطناعي من هذا التهديد، ما يجعل عمليات الاحتيال أكثر خداعاً، وفعاليةً، وصعوبةً في الكشف.

إنتاج محتوى مزيّف ومتنوع

يعتقد إريك بريزكالنز، المحلل والمحرر في «كومسيرك»، أن تأثير الذكاء الاصطناعي على مكالمات الاحتيال مبالغ فيه حالياً، إلا أنه يُشير إلى أن استخدام المحتالين للذكاء الاصطناعي يُركز على إنتاج محتوى مُزيف يبدو حقيقياً، أو على تنويع محتوى الرسائل المُصممة لجذب الضحايا المُحتملين إلى محادثات خبيثة. ويُصرح لصحيفة «فاست كومباني»: «إن تنويع المحتوى يُصعّب تحديد عمليات الاحتيال، وحظرها، باستخدام أدوات مكافحة الاحتيال التقليدية».

أصوات أحبائكم مزيفة

من الأصوات المُزيفة المُولّدة بالذكاء الاصطناعي التي تُحاكي أصوات الأحباء، إلى عمليات الاحتيال واسعة النطاق التي تستخدم التعلم الآلي لتجنب الكشف، يستغل المُجرمون الذكاء الاصطناعي لزيادة فعالية مكالمات الاحتيال هذه. السؤال الأهم هو: كيف يُمكن لقطاع الاتصالات مُكافحة هذه المُشكلة مُباشرةً قبل أن يُسبب المحتالون المزيد من الفوضى؟

وحتى وقت قريب، اعتمدت عمليات الاحتيال الهاتفي في الغالب على المكالمات الآلية المُبسطة -وهي رسائل مُسجلة مُسبقاً تُحذر المُتسلمين من مُشكلة مالية مُلحة، أو مُشكلة مُفترضة في رقم الضمان الاجتماعي الخاص بهم. وهذه الأساليب، رغم استمرارها، يمكن التعرف غالباً بسهولة عليها. لكن عمليات الاحتيال المدعومة بالذكاء الاصطناعي اليوم أكثر إقناعاً بكثير.

احتيال مرعب بـ«استنساخ الصوت»

من أكثر التطورات إثارة للقلق استخدام الأصوات المُولّدة بالذكاء الاصطناعي، ما يجعل عمليات الاحتيال تبدو شخصية بشكل مُقلق. في حالة مُرعبة وقعت في أبريل (نيسان) 2023، تلقت أم في أريزونا مكالمة يائسة من شخص بدا تماماً مثل ابنتها، تبكي وتتوسل طلباً للمساعدة. وطالبها محتال، مُتظاهراً بأنه خاطف، بفدية. في الواقع، كانت الابنة في أمان -فقد استخدم المجرمون الذكاء الاصطناعي لاستنساخ صوتها من فيديو على وسائل التواصل الاجتماعي.

وازدادت عمليات الاحتيال هذه، المعروفة باسم «احتيال استنساخ الصوت»، في الأشهر الأخيرة. فببضع ثوانٍ فقط من الصوت، يُمكن لأدوات الذكاء الاصطناعي الآن إنشاء نسخة رقمية واقعية بشكل مُخيف من صوت الشخص، ما يُمكّن المحتالين من انتحال شخصيات الأصدقاء، أو أفراد العائلة، أو حتى المديرين التنفيذيين في عمليات احتيال الشركات.

صياغة مكالمات موجهة شخصياً

يستخدم المحتالون أيضاً الذكاء الاصطناعي لتحليل كميات هائلة من البيانات، وضبط مخططاتهم بدقة مُرعبة. تستطيع خوارزميات التعلم الآلي غربلة المعلومات العامة -مثل منشورات مواقع التواصل الاجتماعي، والمنتديات الإلكترونية، واختراقات البيانات- لصياغة مكالمات احتيالية مُخصصة للغاية. فبدلاً من خدعة عامة من مصلحة الضرائب، أو الدعم الفني، يمكن للمحتالين الآن استهداف الضحايا بتفاصيل محددة حول مشترياتهم، أو تاريخ سفرهم، أو حتى حالاتهم الطبية.

كما يُعزز الذكاء الاصطناعي عمليات انتحال هوية المتصل، ما يسمح للمحتالين بالتلاعب بأرقام الهواتف لتبدو كأنها صادرة من شركات محلية، أو وكالات حكومية، أو حتى جهات اتصال الضحية. وهذا يزيد من احتمالية رد الناس على المكالمات، ما يجعل تجاهل مكالمات الاحتيال أكثر صعوبة.

الهجوم المضاد لشركات الاتصالات

الذكاء الاصطناعي في مواجهة الذكاء الاصطناعي، هذه هي خلاصة عملية التصدي للاحتيال الإلكتروني. إذ مع صقل المحتالين لأدوات الذكاء الاصطناعي، تُكافح شركات الاتصالات والهيئات التنظيمية باستخدام الذكاء الاصطناعي الخاص بها -من خلال نشر أنظمة متطورة للكشف عن المكالمات الخبيثة، وتتبعها، وحظرها قبل وصولها إلى المستهلكين.

1.التعرف على صدقية المكالمات وكشف الاحتيال باستخدام الذكاء الاصطناعي. لمكافحة انتحال الهوية، تستفيد شركات الاتصالات من تقنيات تحليل الصوت، والمصادقة المدعومة بالذكاء الاصطناعي. وفي الولايات المتحدة، يستخدم إطار عمل STIR/SHAKEN التوقيعات المشفرة للتحقق من أن المكالمات صادرة من مصادر شرعية. ولكن مع تكيف المحتالين السريع، أصبح كشف الاحتيال المدعوم بالذكاء الاصطناعي ضرورياً.

يمكن لنماذج التعلم الآلي المُدربة على مليارات أنماط المكالمات تحليل البيانات الوصفية في الوقت الفعلي للكشف عن أي شذوذ -مثل الارتفاع المفاجئ في المكالمات من مناطق محددة، أو أرقام مرتبطة بعمليات احتيال معروفة. وتستطيع أنظمة الذكاء الاصطناعي هذه حتى اكتشاف العلامات

الصوتية الدقيقة النموذجية للأصوات المُولّدة بتقنية التزييف العميق، ما يُساعد على إيقاف المكالمات الاحتيالية قبل اتصالها.

2.تصفية وترشيح وحظر المكالمات على مستوى شركة الاتصالات. يُدمج كبار مُزودي خدمات الاتصالات تصفية المكالمات المدعومة بالذكاء الاصطناعي مباشرةً في شبكاتهم. مثلاً تستخدم كلٌّ من خدمة Call Protect من شركة «أيه تي أند تي»، وخدمة Scam Shield من شركة «تي - موبايل»، وخدمة Call Filter من «فيريزون» الذكاء الاصطناعي لاكتشاف الأنماط المشبوهة، وحظر المكالمات عالية الخطورة قبل وصولها إلى المستخدمين. كما توفر مرشحات تابعة لشبكة GSMA حماية فورية للمكالمات من خلال التحقق من شرعيتها ومكافحة انتحال هوية خط الاتصال.

1000 خاصية صوتية فريدة للتحقق من الهوية

3. القياسات الحيوية الصوتية المدعومة بالذكاء الاصطناعي للتحقق من هوية المتصل. تُعدّ القياسات الحيوية (البيولوجية) الصوتية خط دفاع واعداً آخر ضد الاحتيال الناتج عن الذكاء الاصطناعي. وتنشر بعض المؤسسات المالية ومقدمو خدمات الاتصالات أنظمة مصادقة صوتية تُحلل أكثر من 1000 خاصية صوتية فريدة للتحقق من هوية المتصل.

وبخلاف تقنية التعرف على الصوت الأساسية، يمكن لهذه الأنظمة المتقدمة اكتشاف وقت استخدام صوت مُولّد بالذكاء الاصطناعي، مما يمنع المحتالين بفعالية من انتحال هوية العملاء الشرعيين.

حملة قانونية صارمة

تشن الهيئات التنظيمية حملة صارمة، ولكن هل هذا كافٍ؟ إن تشديد اللوائح، وتشديد العقوبات أمرٌ واحد، وهو أمرٌ تقوم به بالفعل العديد من الوكالات الحكومية حول العالم، لكن تطبيق هذه اللوائح بفعالية أمرٌ مختلفٌ تماماً. ففي الولايات المتحدة، على سبيل المثال، شددت لجنة الاتصالات الفيدرالية (FCC) العقوبات على المكالمات الآلية غير القانونية، وتحث شركات الاتصالات على اعتماد دفاعات أكثر صرامةً مدعومة بالذكاء الاصطناعي. يمنح قانون TRACED (قانون إنفاذ وردع إساءة استخدام المكالمات الآلية الهاتفية)، الذي تم توقيعه على أنه قانون في عام 2019، الجهات التنظيمية مزيداً من الصلاحيات لتغريم المحتالين، ويفرض تدابير أقوى لمكافحة الانتحال. وعلى الصعيد الدولي، تعمل الجهات التنظيمية في المملكة المتحدة وكندا وأستراليا على أطر عمل مماثلة تعتمد على الذكاء الاصطناعي لحماية المستهلكين من الاحتيال المتزايد. وقد أصدر الاتحاد الأوروبي قوانين أكثر صرامة بشأن خصوصية البيانات، ما يحد من كيفية استخدام الذكاء الاصطناعي لجمع البيانات الشخصية لعمليات الاحتيال.

ومع ذلك، فإن جهات إنفاذ القانون تكافح لمواكبة سرعة ابتكار الذكاء الاصطناعي. ويعمل المحتالون على مستوى العالم، وغالباً ما يكونون خارج نطاق اختصاص أي جهة تنظيمية واحدة. تتمركز العديد من شبكات الاحتيال في بلدان يصعب فيها اتخاذ إجراءات قانونية، إن لم يكن شبه مستحيل.

لنأخذ، على سبيل المثال، دولاً مثل ميانمار، وكمبوديا، ولاوس، حيث أنشأت جماعات الجريمة المنظمة مراكز احتيال إلكتروني تستخدم تقنيات التزييف العميق المدعومة بالذكاء الاصطناعي لخداع الضحايا حول العالم. وكثيراً ما ينقل مشغلو هذه المراكز مواقعهم، أو يغيرون أساليبهم للبقاء في صدارة جهات إنفاذ القانون. كما أنهم يعملون في مناطق تواجه تحديات قضائية معقدة، ما يزيد من تعقيد عملية إنفاذ القانون.

عوائق تنظيمية

يزدهر المحتالون في ظل التشتت، واستغلال نقاط الضعف، سواءً كان ذلك نقصاً في التنسيق بين القطاعات، أو اختلافاً في النهج التنظيمية عبر الحدود. تُبرز هذه العوائق التنظيمية ضرورة قيام مزودي خدمات الاتصالات بدور أكثر استباقية في مكافحة الاحتيال المدعوم بالذكاء الاصطناعي، بدلاً من الاعتماد فقط على الأطر التقليدية التي -رغم فائدتها- ليست دائماً فعالة. وهنا يأتي دور تقنية GSMA Call Check، التي طورتها شركة «أوكيلوس» Oculeus الألمانية لحلول الاتصالات، في تحقيق هدفها الحيوي. تُوفر خدمات التحقق من المكالمات من GSMA آلية بسيطة، وسريعة، ومنخفضة التكلفة لتبادل المعلومات حول مكالمات الهاتف الاحتيالية فور حدوثها. يقول بريزكالنز من «كوميرسك» إن «هذه التقنية مُتجذرة في السحابة، ما يجعلها مُستقبلية، وعالمية بطريقة لن تكون عليها أبداً الطرق الأخرى التي تُفكر فيها بعض الدول».

معركة طويلة

لا شك أن المعركة ضد عمليات الاحتيال المُدعمة بالذكاء الاصطناعي لم تنتهِ بعد. وكما أشارت جيسيكا روزينورسيل، رئيسة لجنة الاتصالات الفيدرالية (FCC) السابقة، العام الماضي: «نعلم أن تقنيات الذكاء الاصطناعي ستجعل من السهل والرخيص إغراق شبكاتنا بمقاطع فيديو مُزيفة تُستخدم للتضليل، وزعزعة الثقة».

الخبر السار هو أن قطاع الاتصالات لا يتراجع، فبينما يستخدم المحتالون الذكاء الاصطناعي لخداع الأفراد غير المُنتبهين، فإن القطاع يستفيد أيضاً من الذكاء الاصطناعي لحماية العملاء وبياناتهم الحساسة، من خلال فحص المكالمات الآلي، والكشف الفوري عن الاحتيال، وإجراءات المصادقة المُحسّنة.

أمر واحد مؤكد: المحتالون وعمليات الاحتيال لن تختفي في أي وقت قريب. وكما يشير بريزكالنز، سيستمر الناس في الوقوع ضحية عمليات الاحتيال حتى مع التدريب المكثف على التوعية العامة. ولكن مع استمرار تطور الذكاء الاصطناعي، يجب على قطاع الاتصالات أن يكون متقدماً بخطوة، لضمان أن يصبح قوة للحماية، لا للخداع.

* مجلة «فاست كومباني» خدمات «تريبيون ميديا»

مواضيع

الذكاء الاصطناعي

العالم